

# STRONGLY ÉTALE DIFFERENCE ALGEBRAS AND BABBITT'S DECOMPOSITION

IVAN TOMAŠIĆ AND MICHAEL WIBMER

**ABSTRACT.** We introduce a class of *strongly étale difference algebras*, whose role in the study of difference equations is analogous to the role of étale algebras in the study of algebraic equations. We deduce an improved version of Babbitt's decomposition theorem and we present applications to difference algebraic groups and the compatibility problem.

## INTRODUCTION

**Strongly  $\sigma$ -étale algebras and strong core.** Étale algebras play an important role in commutative algebra and algebraic geometry. In this paper we initiate the study of suitable notions of *étale* in difference algebra and geometry by introducing *strongly  $\sigma$ -étale difference algebras* as difference algebras that are (algebraically) étale and  $\sigma$ -separable. We develop a comprehensive understanding of the class of difference algebras they constitute, and consequently we establish their rugged permanence properties.

We define the *strong core* of a difference algebra  $R$  over a difference field  $k$  as the union

$$\pi_0^\sigma(R|k)$$

of all strongly  $\sigma$ -étale difference subalgebras of  $R$ , and we show that it has good functorial properties. In particular, the formation of the strong core is compatible with the tensor product and extension of the base difference field.

Strongly  $\sigma$ -étale difference algebras are the best behaved among the variety of notions of étale extensions of difference rings studied in [Tom16] (étale extensions of finite  $\sigma$ -type and ind- $\sigma$ -étale extensions, with or without the  $\sigma$ -separability assumption) and [Tom14] (directly-étale extensions). These more general notions will be studied in our forthcoming work.

**Improved Babbitt's decomposition.** The framework of strongly  $\sigma$ -étale difference algebras and the strong core allows us to prove an enhanced variant of Babbitt's decomposition, one of the most important structure theorems in difference algebra. Babbitt's theorem was instrumental for extending specializations and in the study of compatibility of difference field extensions, see [Lev08, Section 5.4]. It has also been used in [CHP02], as well as [Tom16] and [Tom15].

The original Babbitt's decomposition (see [Bab62, Theorem 2.3] or [Lev08, Theorem 5.4.13]) applies to finitely generated extensions of difference fields  $L|K$  such that  $K$  is inversive and the field extension  $L|K$  is Galois.

The assumption that the base difference field  $K$  is inversive is used in several steps of the known proofs of Babbitt's decomposition theorem and is somewhat of a hindrance for applying the theorem. We show here that the assumption that the base difference field is inversive can be dropped. This generalization is achieved by replacing the core of  $L|K$  with the strong core  $\pi_0^\sigma(L|K)$ .

---

The authors would like to thank the London Mathematical Society for supporting our work through a *Research in Pairs* grant.

By definition, for an arbitrary extension of difference fields  $L|K$ , the core of  $L|K$  contains  $\pi_0^\sigma(L|K)$ . On the other hand, we show that the core  $\sigma$ -radical over the strong core.

Un upshot is that we can shed light on the classical problem of compatibility of difference field extensions. The classical compatibility theorem (see [Lev08, Theorem 5.4.22]) states that two extensions of difference fields  $L|K$  and  $L'|K$  are compatible if and only if their cores are compatible. We can actually show that  $L|K$  and  $L'|K$  are compatible if and only if  $\pi_0^\sigma(L|K)$  and  $\pi_0^\sigma(L'|K)$  are compatible.

**Difference algebraic groups and connected components.** If  $G$  is an (affine) algebraic group over a field  $k$ , then the union  $\pi_0(k[G])$  of all étale  $k$ -subalgebras of the coordinate ring  $k[G]$  of  $G$  is a Hopf-subalgebra of  $k[G]$  that represents the quotient  $G/G^\circ$  of  $G$  by the connected component  $G^\circ$  of  $G$ . Indeed, one may use  $\pi_0(k[G])$  to define  $G^\circ$  (see [Wat79, Section 6.7], [Mil12, Chapter XIII, Def. 3.1]).

Our initial motivation for studying the difference analog of étale algebras was the desire to define the *difference connected component* of an (affine) difference algebraic group  $G$ , i.e.,  $G$  is a group defined by algebraic difference equations. If  $R$  is a difference Hopf algebra over a difference field  $k$ , the union of all difference subalgebras of  $R$  that are étale as  $k$ -algebras need not be a Hopf subalgebra of  $R$ , as shown in Example 3.4. In this article, however, we show that  $\pi_0^\sigma(R)$  is a Hopf subalgebra of  $R$ . This paves the way for the definition of the difference connected component of a difference algebraic group, see [Wib15, Section 4.2].

**Structure of the paper.** Let us describe the content of the article in more detail. In Section 1, we discuss  $\sigma$ -separability, introduce strongly  $\sigma$ -étale difference algebras and establish their basic properties. We define the strong core and show its functorial properties. Finally, we explain the relation between  $\pi_0^\sigma(L|K)$  and the core of a difference field extension  $L|K$ .

In Section 2 we establish the improved version of Babbitt's decomposition theorem (Theorem 2.8).

Section 3 is devoted to applications of the developed theory.

- (i) As a contribution to the study of difference connected components of difference algebraic groups, we show that  $\pi_0^\sigma(R|k)$  is a Hopf subalgebra if  $R$  is a difference Hopf algebra, respecting the appropriate finiteness properties.
- (ii) Elaborating on the classical theory of difference field extensions, we present an application of our work to the compatibility problem.

## 1. STRONGLY $\sigma$ -ÉTALE DIFFERENCE ALGEBRAS

We start by recalling the basic definitions and conventions from difference algebra. Standard references for difference algebra are [Lev08] and [Coh65]. All rings are assumed to be commutative. A *difference ring* (or  $\sigma$ -ring for short) is a ring  $R$  together with a ring endomorphism  $\sigma: R \rightarrow R$ . A *morphism of  $\sigma$ -rings*  $R$  and  $S$  is a morphism  $\psi: R \rightarrow S$  of rings such that

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \sigma \downarrow & & \downarrow \sigma \\ R & \xrightarrow{\psi} & S \end{array}$$

commutes. In this situation, we also say that  $S$  is an  $R$ - $\sigma$ -algebra. Note that in contrast to [Lev08] and [Coh65] we do not require  $\sigma: R \rightarrow R$  to be injective. A  $\sigma$ -ring  $R$  with  $\sigma: R \rightarrow R$  injective is called  $\sigma$ -reduced. If  $\sigma: R \rightarrow R$  is an automorphism,  $R$  is called *inversive*.

If  $R$  and  $S$  are  $\sigma$ -rings such that  $R$  is a subring of  $S$  and the inclusion map is a morphism of  $\sigma$ -rings, we say that  $R$  is a  $\sigma$ -subring of  $S$ .

A *difference field* (or  $\sigma$ -field for short) is a difference ring whose underlying ring is a field. If  $K$  and  $L$  are  $\sigma$ -fields such that  $K$  is a  $\sigma$ -subring of  $L$ , we also say that  $L$  is a  $\sigma$ -field extension of  $K$ , or that  $L|K$  is an *extension of  $\sigma$ -fields*, or that  $K$  is a  $\sigma$ -subfield of  $L$ .

Let  $L|K$  be an extension of  $\sigma$ -fields and  $F \subset L$  a subset. The smallest  $\sigma$ -subfield of  $L$  that contains  $K$  and  $F$  is denoted by

$$K\langle F \rangle.$$

As a field extension of  $K$  the  $\sigma$ -field  $K\langle F \rangle$  is generated by all elements of the form  $\sigma^i(f)$  with  $i \in \mathbb{N}$  and  $f \in F$ . We call  $K\langle F \rangle$  the  $\sigma$ -field  $\sigma$ -generated by  $F$  over  $K$ . If  $L = K\langle F \rangle$  for a finite subset  $F$  of  $L$  we say that  $L$  is *finitely  $\sigma$ -generated as a  $\sigma$ -field extension of  $K$* .

Let  $k$  be a difference ring. A *morphism of  $k$ - $\sigma$ -algebras* is a morphism of  $k$ -algebras that is also a morphism of  $\sigma$ -rings. If  $R$  and  $S$  are  $k$ - $\sigma$ -algebras  $R \otimes_k S$  is naturally a  $\sigma$ -ring by  $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$  for  $r \in R$  and  $s \in S$ .

A  $k$ - $\sigma$ -subalgebra of a  $k$ - $\sigma$ -algebra  $R$  is a  $k$ -subalgebra of  $R$  that is also  $\sigma$ -subring of  $R$ . For a subset  $F \subset R$ , the smallest  $k$ - $\sigma$ -subalgebra of  $R$  that contains  $F$  is denoted by

$$k\{F\}.$$

It is called the  $k$ - $\sigma$ -subalgebra of  $R$   $\sigma$ -generated by  $F$  (over  $k$ ). As a  $k$ -algebra,  $k\{F\}$  is generated by all elements of the form  $\sigma^i(f)$  with  $i \in \mathbb{N}$  and  $f \in F$ . A  $k$ - $\sigma$ -algebra  $R$  is called *finitely  $\sigma$ -generated* (over  $k$ ) if there exists a finite set  $F \subset R$  such that  $R = k\{F\}$ .

Let  $k$  be a  $\sigma$ -field and  $R$  a  $k$ - $\sigma$ -algebra. Note that  $\sigma: k \rightarrow k$  is a morphism of difference rings. We denote by

$${}^\sigma R$$

the  $k$ - $\sigma$ -algebra obtained from  $R$  by extension of scalars via  $\sigma: k \rightarrow k$ , i.e.,  ${}^\sigma R = R \otimes_k k$  with  $k$ -algebra structure map  $k \rightarrow {}^\sigma R$  given by  $\lambda \mapsto 1 \otimes \lambda$ .

For a difference ring  $R$ , we denote its *inversive closure* (see [Lev08, Def. 2.1.6]) by  $R^*$ . If  $f$  is a univariate polynomial with coefficients in some field, and  $\tau$  is an endomorphism on that field, we denote by

$$\tau f$$

the polynomial obtained from  $f$  by applying  $\tau$  to the coefficients.

**1.1.  $\sigma$ -separable  $\sigma$ -algebras.** *From now on we assume that  $k$  is a difference field.*

The notion of a  $\sigma$ -separable  $\sigma$ -algebra does not appear in the standard textbooks [Coh65] and [Lev08], but it has proved useful in recent literature, including [Hru04, Section 5.1], [Wib10, Section 1.5], [DVHW14, Section 4] and [Tom16], [Tom15]. In this subsection we collect basic properties of  $\sigma$ -separable  $\sigma$ -algebras that will be needed later.

**Definition 1.1.** *A  $k$ - $\sigma$ -algebra  $R$  is called  $\sigma$ -separable (over  $k$ ) if  $R \otimes_k K$  is  $\sigma$ -reduced for every  $\sigma$ -field extension  $K|k$ .*

Note that Definition 1.1 generalizes the notion of a separable algebra. (See Corollary 1.3 for a precise mathematical statement.)

**Proposition 1.2.** *The following conditions on a  $k$ - $\sigma$ -algebra  $R$  are equivalent:*

- (i)  $R$  is  $\sigma$ -separable over  $k$ .
- (ii)  $R \otimes_k K$  is  $\sigma$ -reduced, where  $K = k^*$  denotes the inversive closure of  $k$ .
- (iii)  $R \otimes_k K$  is  $\sigma$ -reduced for some inversive  $\sigma$ -field extension  $K$  of  $k$ .

- (iv) If  $f_1, \dots, f_n \in R$  are  $k$ -linearly independent, then also  $\sigma(f_1), \dots, \sigma(f_n) \in R$  are  $k$ -linearly independent.
- (v) The canonical map  ${}^\sigma R = R \otimes_k k \rightarrow R$ ,  $f \otimes \lambda \mapsto \sigma(f)\lambda$  is injective.
- (vi)  $R$  is  $\sigma$ -reduced and linearly disjoint from  $k^*$  over  $k$  (inside  $R^*$ ).
- (vii)  $R \otimes_k S$  is  $\sigma$ -reduced for every  $\sigma$ -reduced  $k$ - $\sigma$ -algebra  $S$ .

*Proof.* Cf. Proposition 1.5.2 in [Wib10] and Theorem 2, Chapter V, §15, No. 4 in [Bou90]. The implications (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) are trivial. Let us show that (iii) implies (iv). Assume  $\lambda_1\sigma(f_1) + \dots + \lambda_n\sigma(f_n) = 0$  with  $\lambda_1, \dots, \lambda_n \in k$ . Because  $K$  is inersive, there exist  $\mu_1, \dots, \mu_n \in K$  with  $\sigma(\mu_i) = \lambda_i$  for  $i = 1, \dots, n$ . Then

$$\sigma\left(\sum f_i \otimes \mu_i\right) = \sum \sigma(f_i) \otimes \lambda_i = 0 \in R \otimes_k K.$$

Because  $R \otimes_k K$  is  $\sigma$ -reduced and the  $f_i$ 's are  $k$ -linearly independent, this implies that  $\mu_i = 0$  for  $i = 1, \dots, n$ . Thus  $\lambda_i = \sigma(\mu_i) = 0$  for  $i = 1, \dots, n$ .

Clearly (iv) and (v) are equivalent. Next we will show that (iv) implies (vi). If  $f \in R$  is non-zero,  $\sigma(f)$  is  $k$ -linearly independent and thus non-zero. So  $R$  is  $\sigma$ -reduced. Let  $f_1, \dots, f_n \in R \subset R^*$  be  $k$ -linearly independent and assume that  $\lambda_1, \dots, \lambda_n \in k^*$  are such that  $\lambda_1 f_1 + \dots + \lambda_n f_n = 0$ . Then there is some  $m \geq 1$  such that  $\sigma^m(\lambda_i) \in k$  for  $i = 1, \dots, n$ . So  $\sigma^m(\lambda_1)\sigma^m(f_1) + \dots + \sigma^m(\lambda_n)\sigma^m(f_n) = 0$  is a linear dependence relation for  $\sigma^m(f_1), \dots, \sigma^m(f_n)$  over  $k$ . By (iv) it must be trivial. So  $\sigma^m(\lambda_i) = 0$  and therefore  $\lambda_i = 0$ .

To see that (vi) implies (iv), assume that  $f_1, \dots, f_n \in R$  are  $k$ -linearly independent and let  $\lambda_1, \dots, \lambda_n \in k$  with  $\lambda_1\sigma(f_1) + \dots + \lambda_n\sigma(f_n) = 0$ . Let  $\mu_i \in k^*$  with  $\sigma(\mu_i) = \lambda_i$ . Then  $\sigma(\mu_1 f_1 + \dots + \mu_n f_n) = 0$ . But  $\mu_1 f_1 + \dots + \mu_n f_n \in R^*$  and thus  $\mu_1 f_1 + \dots + \mu_n f_n = 0$ . So the  $\mu_i$ 's and therefore also the  $\lambda_i$ 's are zero.

Next we will show that (iv) implies (vii). Assume that  $f \in R \otimes_k S$  with  $\sigma(f) = 0$ . Let  $(f_i)$  be a  $k$ -basis of  $R$ . Then  $f = \sum f_i \otimes s_i$  with  $s_i \in S$  and  $\sum \sigma(f_i) \otimes \sigma(s_i) = \sigma(f) = 0$ . Because the  $\sigma(f_i)$ 's are  $k$ -linearly independent we have  $\sigma(s_i) = 0$  for all  $i$ . But as  $S$  is  $\sigma$ -reduced this implies that  $s_i = 0$  and therefore  $f = 0$ .

Finally the implication (vi) $\Rightarrow$ (i) is trivial.  $\square$

**Corollary 1.3.** *Let  $k$  be field of positive characteristic  $p$  and let  $q$  be a power of  $p$ . Let  $R$  be a  $k$ -algebra and consider  $k$  and  $R$  as difference rings via the Frobenius endomorphism, i.e.,  $\sigma(f) = f^q$  for  $f \in R$ . Then  $R$  is  $\sigma$ -separable over  $k$  if and only if  $R$  is a separable  $k$ -algebra.*

*Proof.* Assume that  $R$  is  $\sigma$ -separable over  $k$  and let  $K$  be a field extension of  $k$ . We have to show that  $R \otimes_k K$  is reduced. But if we consider  $K$  as a  $\sigma$ -field via  $\sigma(f) = f^q$ , then, by assumption,  $\sigma$  is injective on  $R \otimes_k K$ . Thus  $R \otimes_k K$  is reduced.

Conversely, assume that  $R$  is a separable  $k$ -algebra. By [Bou90, Theorem 2, Chapter V, §15, No. 4, A.V.123] the elements  $f_1^p, \dots, f_n^p$  are  $k$ -linearly independent if  $f_1, \dots, f_n \in R$  are  $k$ -linearly independent. Therefore  $\sigma(f_1), \dots, \sigma(f_n)$  are  $k$ -linearly independent and it follows from Proposition 1.2 that  $R$  is  $\sigma$ -separable over  $k$ .  $\square$

**Corollary 1.4.** *If  $R$  and  $S$  are  $\sigma$ -separable  $k$ - $\sigma$ -algebras, then also  $R \otimes_k S$  is a  $\sigma$ -separable  $k$ - $\sigma$ -algebra.*

*Proof.* Let  $K$  be a  $\sigma$ -field extension of  $k$ . Then  $S \otimes_k K$  is  $\sigma$ -reduced because  $S$  is  $\sigma$ -separable. Therefore  $(R \otimes_k S) \otimes_k K = R \otimes_k (S \otimes_k K)$  is  $\sigma$ -reduced by Proposition 1.2.  $\square$

**Corollary 1.5.** *Let  $R$  be a  $k$ - $\sigma$ -algebra and  $K$  a  $\sigma$ -field extension of  $k$ . Then  $R$  is  $\sigma$ -separable over  $k$  if and only if  $R \otimes_k K$  is  $\sigma$ -separable over  $K$ .*

*Proof.* Let us first assume that  $R$  is  $\sigma$ -separable over  $k$ . Let  $L$  be a  $\sigma$ -field extension of  $K$ . Then  $(R \otimes_k K)_K L = R \otimes_k L$  is  $\sigma$ -reduced. Thus  $R \otimes_k K$  is  $\sigma$ -separable over  $K$ .

Conversely, if  $R \otimes_k K$  is  $\sigma$ -separable over  $K$ , it follows that  $(R \otimes_k K) \otimes_K K^* = R \otimes_k K^*$  is  $\sigma$ -reduced. Thus  $R$  is  $\sigma$ -separable over  $k$  by Proposition 1.2.  $\square$

**Corollary 1.6.** *Let  $K|k$  be an extension of  $\sigma$ -fields. If  $k$  is inversive, then  $K$  is  $\sigma$ -separable over  $k$ .*

*Proof.* By Proposition 1.2 it suffices to note that a  $\sigma$ -field is  $\sigma$ -reduced.  $\square$

**1.2. Strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebras.** In this subsection we introduce strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebras and establish their basic properties.

Recall ([Bou90, Chapter V, §6]) that an algebra  $R$  over a field  $k$  is called étale if  $R \otimes_k \bar{k}$  is isomorphic to a finite direct product of copies of the algebraic closure  $\bar{k}$  of  $k$ . (In particular,  $R$  is finite dimensional as a  $k$ -vector space.) The following definition introduces a difference analog of étale algebras.

**Definition 1.7.** *A  $k$ - $\sigma$ -algebra is called strongly  $\sigma$ -étale if it is  $\sigma$ -separable over  $k$  and étale as a  $k$ -algebra.*

Note that by Proposition 1.2, over an inversive  $\sigma$ -field  $k$ , a  $k$ - $\sigma$ -algebra whose underlying  $k$ -algebra is étale is strongly  $\sigma$ -étale if and only if it is inversive.

**Lemma 1.8.** *Let  $R$  be a  $k$ - $\sigma$ -algebra and  $K$  a  $\sigma$ -field extension of  $k$ . Then  $R$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra if and only if  $R \otimes_k K$  is a strongly  $\sigma$ -étale  $K$ - $\sigma$ -algebra.*

*Proof.* By [Wat79, Cor. 6.2, p. 47] or [Bou90, Cor. 2, Chapter V, §6, No. 5, A.V.32] the  $k$ -algebra  $R$  is étale if and only if the  $K$ -algebra  $R \otimes_k K$  is étale. Similarly, by Corollary 1.5 the  $k$ - $\sigma$ -algebra  $R$  is  $\sigma$ -separable if and only if the  $K$ - $\sigma$ -algebra  $R \otimes_k K$  is  $\sigma$ -separable.  $\square$

Let  $R$  be a  $\sigma$ -ring. Following [Lev08] an element  $f \in R$  is called *periodic* if  $\sigma^n(f) = f$  for some  $n \geq 1$ .

**Lemma 1.9.** *Let  $R$  be a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra. Then  $\sigma$  induces a bijection on the set of primitive idempotent elements of  $R$ . Moreover, every idempotent element of  $R$  is periodic.*

*Proof.* Let  ${}^\sigma R = R \otimes_k k$  be the  $k$ - $\sigma$ -algebra obtained from  $R$  by base extension via  $\sigma: k \rightarrow k$ . Because  $R$  is  $\sigma$ -separable over  $k$ , it follows from Proposition 1.2 that

$$\psi: {}^\sigma R = R \otimes_k k \rightarrow R, f \otimes \lambda \mapsto \sigma(f)\lambda$$

is injective. As  $R$  is a finite dimensional  $k$ -vector space, this implies that  $\psi$  is an isomorphism of  $k$ -algebras. Let  $e_1, \dots, e_n$  denote the primitive idempotent elements of  $R$ . Then there are precisely  $n$  primitive idempotent elements in  ${}^\sigma R$ . These must be  $e_1 \otimes 1, \dots, e_n \otimes 1 \in {}^\sigma R = R \otimes_k k$  and they are mapped bijectively onto the  $e_i$ 's under  $\psi$ . This shows that  $e \mapsto \sigma(e)$  defines a bijection on  $\{e_1, \dots, e_n\}$ . In particular, each  $e_i$  is periodic. Since an arbitrary idempotent element of  $R$  is a sum of certain  $e_i$ 's, it follows that any idempotent element of  $R$  is periodic.  $\square$

**Lemma 1.10.** *A  $k$ - $\sigma$ -algebra  $\sigma$ -generated by finitely many periodic idempotent elements is strongly  $\sigma$ -étale.*

*Proof.* Let  $R$  be  $k$ - $\sigma$ -algebra  $\sigma$ -generated by finitely many periodic idempotent elements. Because the  $\sigma$ -generators are periodic,  $R$  is in fact generated as a  $k$ -algebra by finitely many idempotent elements. For a non-trivial idempotent element  $e \in R$  we have  $k[e] \simeq k \times k$ , which is an étale  $k$ -algebra. Thus a  $k$ -algebra generated by finitely many idempotent elements can be written as a quotient of a finite tensor product of étale  $k$ -algebras. Since quotients and tensor products

of étale  $k$ -algebras are étale ([Bou90, Chapter V, §6]) it follows that  $R$  is étale. Moreover,  $R$  is generated as a  $k$ -vector space by periodic idempotent elements.

To show that  $R$  is  $\sigma$ -separable over  $k$  it suffices to show that

$$\psi: {}^\sigma R = R \otimes_k k \rightarrow R, r \otimes \lambda \mapsto \lambda \sigma(r)$$

is injective (Proposition 1.2). Let  $e_1, \dots, e_n$  be the primitive idempotent elements in  $R$ . These are a  $k$ -basis of  $R$  and therefore  $e_1 \otimes 1, \dots, e_n \otimes 1 \in R \otimes_k k$  is a  $k$ -basis of  ${}^\sigma R$ . Moreover, the primitive idempotent elements in  ${}^\sigma R$  are  $e_1 \otimes 1, \dots, e_n \otimes 1$ . Thus every idempotent element in  ${}^\sigma R$  is of the form  $e \otimes 1$  for some idempotent element  $e \in R$ . Every ideal in  ${}^\sigma R$  is generated by an idempotent element. Therefore the kernel of  $\psi$  is generated by an element of the form  $e \otimes 1$ , where  $e \in R$  is idempotent. So  $\sigma(e) = 0$ .

There exists a  $k$ -basis  $d_1, \dots, d_n$  of  $R$  consisting of periodic idempotent elements. We can find an integer  $m \geq 1$  such that  $\sigma^m(d_i) = d_i$  for  $i = 1, \dots, n$ . We may write  $e = \lambda_1 d_1 + \dots + \lambda_n d_n$  for  $\lambda_1, \dots, \lambda_n \in k$ . Then

$$0 = \sigma^m(e) = \sigma^m(\lambda_1) d_1 + \dots + \sigma^m(\lambda_n) d_n.$$

Therefore  $\sigma^m(\lambda_1) = \dots = \sigma^m(\lambda_n) = 0$  and consequently also  $e = 0$ . This shows that  $\psi$  is injective.  $\square$

It is sometimes convenient to be able to assume that the base  $\sigma$ -field  $k$  is algebraically closed or separably algebraically closed. This can be achieved by passing to the (separable) algebraic closure. In this respect the following remark is relevant.

**Remark 1.11.** *Let  $k$  be a  $\sigma$ -field and let  $\bar{k}$  denote an algebraic closure of  $k$ . Then  $\sigma: k \rightarrow k$  can be extended to an endomorphism  $\sigma: \bar{k} \rightarrow \bar{k}$ . The separable algebraic closure  $k_s \subset \bar{k}$  of  $k$  is stable under  $\sigma$ . In particular,  $\sigma: k \rightarrow k$  can be extended to an endomorphism on the separable algebraic closure of  $k$ .*

*Proof.* By [Lev08, Corollary 5.1.16] there exists an extension  $\sigma: \bar{k} \rightarrow \bar{k}$  of  $\sigma: k \rightarrow k$ .

Recall, for a polynomial  $f$  with coefficients in  $k$ , we write  ${}^\sigma f$  for the polynomial obtained by applying  $\sigma$  to the coefficients of  $f$ . If 1 lies in the ideal generated by  $f$  and its formal derivative, then 1 also lies in the ideal generated by  ${}^\sigma f$  and its formal derivative. Thus,  ${}^\sigma f$  is separable if  $f$  is separable. If  $a \in \bar{k}$  is a solution of  $f$ , then  $\sigma(a)$  is a solution of  ${}^\sigma f$ . Therefore  $\sigma(k_s) \subset k_s$ .  $\square$

The following proposition provides a partial converse to the last lemma.

**Proposition 1.12.** *The  $R$  be a  $k$ - $\sigma$ -algebra that is finite dimensional as a  $k$ -vector space. Let  $k_s$  denote the separable algebraic closure of  $k$ , equipped with an extension of  $\sigma: k \rightarrow k$ . Then  $R$  is strongly  $\sigma$ -étale if and only if  $R \otimes_k k_s$  is generated as a  $k_s$ -vector space by periodic idempotent elements.*

*Proof.* By Lemma 1.8 we may assume  $k = k_s$ .

Let us first assume that  $R$  is strongly  $\sigma$ -étale. Since  $k = k_s$  and  $R$  is an étale  $k$ -algebra,  $R$  is generated as a  $k$ -vector space by idempotent elements (cf. [Wat79, Theorem 6.2]). By Lemma 1.9 every idempotent element of  $R$  is periodic.

Conversely, if  $R$  is generated by periodic idempotent elements, then it follows from Lemma 1.10 that  $R$  is strongly  $\sigma$ -étale.  $\square$

**Lemma 1.13.** (i) *A  $k$ - $\sigma$ -subalgebra of a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra is strongly  $\sigma$ -étale.*  
(ii) *The tensor product of two strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebras is strongly  $\sigma$ -étale.*  
(iii) *The quotient of a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra by a  $\sigma$ -ideal is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra.*

*Proof.* The first statement follows from the fact that a  $k$ -subalgebra of an étale  $k$ -algebra is étale ([Bou90, Prop. 3, Chapter V, §6, No. 4, A.V.30]) and the obvious fact that a  $k$ - $\sigma$ -subalgebra of a  $\sigma$ -separable  $k$ - $\sigma$ -algebra is  $\sigma$ -separable.

The second statement follows from the fact that the tensor product of two étale  $k$ -algebras is étale ([Bou90, Cor. 1, Chapter V, §6, No. 5, A.V.32]) and the fact that the tensor product of two  $\sigma$ -separable  $k$ - $\sigma$ -algebras is  $\sigma$ -separable (Corollary 1.4).

Finally we prove the third statement. Let  $R$  be a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra and  $\mathfrak{a}$  a  $\sigma$ -ideal of  $R$ . Let  $k_s$  denote the separable algebraic closure of  $k$ , equipped with an extension of  $\sigma$ , as per Remark 1.11. Then

$$(R/\mathfrak{a}) \otimes_k k_s = (R \otimes_k k_s) / (\mathfrak{a} \otimes_k k_s).$$

It follows from Proposition 1.12, that the right-hand side is generated as a  $k_s$ -vector space by periodic idempotent elements. Applying the proposition again yields the conclusion.  $\square$

The following lemma shows that being strongly  $\sigma$ -étale is transitive.

**Lemma 1.14.** *Let  $K|k$  be a strongly  $\sigma$ -étale  $\sigma$ -field extension, i.e.,  $K$  is a finite, separable,  $\sigma$ -separable  $\sigma$ -field extension of  $k$ . Let  $R$  be a strongly  $\sigma$ -étale  $K$ - $\sigma$ -algebra. Then  $R$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra.*

*Proof.* Since  $R$  is an étale  $K$ -algebra and  $K$  is an étale  $k$ -algebra it follows from [Bou90, Cor. 2 (b), A.V.32] that  $R$  is an étale  $k$ -algebra. Thus it suffices to show that  $R$  is  $\sigma$ -separable over  $k$ . So we have to show that the map

$$\begin{aligned} \psi: {}^\sigma R &= R \otimes_k k \rightarrow R \\ r \otimes \lambda &\mapsto \sigma(r)\lambda \end{aligned}$$

is injective. Because  $R$  is a finite dimensional  $k$ -vector space and  $\psi$  is  $k$ -linear, it suffices to show that  $\psi$  is surjective. So let  $r \in R$ . By assumption the canonical maps  $R \otimes_K K \rightarrow R$  and  $K \otimes_k k \rightarrow K$  are injective and thus surjective. So we can write  $r = \sum \sigma(r_i)\mu_i$  with  $r_i \in R$  and  $\mu_i \in K$ . Similarly, we can write  $\mu_i = \sum \sigma(a_{ij})\lambda_{ij}$  with  $a_{ij} \in K$  and  $\lambda_{ij} \in k$ . Then

$$r = \sum_{i,j} \sigma(r_i a_{ij}) \lambda_{ij}$$

lies in the image of  $\psi$ .  $\square$

### 1.3. The strong core.

**Definition 1.15.** *Let  $R$  be a  $k$ - $\sigma$ -algebra. We define the strong core*

$$\pi_0^\sigma(R) = \pi_0^\sigma(R|k)$$

*as the union of all strongly  $\sigma$ -étale  $k$ - $\sigma$ -subalgebras of  $R$ .*

In this section we show that this construction has good functorial properties.

**Remark 1.16.** *We have that  $\pi_0^\sigma(R)$  is a  $\sigma$ -separable  $k$ - $\sigma$ -subalgebra of  $R$ . Indeed, if  $R_1$  and  $R_2$  are strongly  $\sigma$ -étale  $k$ - $\sigma$ -subalgebras of a  $k$ - $\sigma$ -algebra  $R$ , then also  $R_1 R_2$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra by Lemma 1.13, since  $R_1 R_2$  may be written as a quotient of  $R_1 \otimes_k R_2$ .*

Note that  $\pi_0^\sigma(R)$  need not be strongly  $\sigma$ -étale in general. Indeed,  $\pi_0^\sigma(R)$  is strongly  $\sigma$ -étale if and only if  $\pi_0^\sigma(R)$  is finitely  $\sigma$ -generated over  $k$ . This is also equivalent to  $\pi_0^\sigma(R)$  being finite dimensional as a  $k$ -vector space.

**Conjecture 1.17.** *If  $R$  is a finitely  $\sigma$ -generated  $k$ - $\sigma$ -algebra, then  $\pi_0^\sigma(R)$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra.*

We will see later (Theorem 3.2) that  $\pi_0^\sigma(R)$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -subalgebra of  $R$  if  $R$  is a finitely  $\sigma$ -generated  $k$ - $\sigma$ -Hopf algebra.

**Lemma 1.18.** *Let  $R$  be a  $k$ - $\sigma$ -algebra. If  $k$  is separably algebraically closed, then  $\pi_0^\sigma(R)$  is the  $k$ -subvector space of  $R$  generated by all periodic idempotent elements of  $R$ .*

*Proof.* It is clear from Proposition 1.12 that  $\pi_0^\sigma(R)$  is contained in the  $k$ -subvector space of  $R$  generated by all periodic idempotent elements of  $R$ .

On the other hand,  $k\{e\} \subset \pi_0^\sigma(R)$  for every periodic idempotent element  $e \in R$  by Lemma 1.10.  $\square$

We will need a simple algebraic (rather than difference algebraic) lemma on idempotent elements.

**Lemma 1.19.** *Let  $k$  be an algebraically closed field,  $K$  a field extension of  $k$  and  $R$  a  $k$ -algebra. Then every idempotent element  $e$  of  $R \otimes_k K$  is of the form  $e = f \otimes 1$  for some idempotent element  $f \in R$ .*

*Proof.* A field extension of an algebraically closed field is geometrically connected (in the sense of Definition [Sta14, Tag 037T]). The claim thus follows from [Sta14, Tag 037W].  $\square$

Our next important goal is to show that the formation of  $\pi_0^\sigma$  is compatible with extension of the base  $\sigma$ -field. To prove this for the extension  $k_s|k$ , where  $k_s$  denotes the separable algebraic closure of  $k$  we will use Galois descent. In this connection we need to introduce an action of  $\sigma$  on the absolute Galois group of  $k$ . To define this action we need a simple lemma on field extensions. We include the proof for the sake of completeness.

**Lemma 1.20.** *Let  $K$  be a  $\sigma$ -field,  $L$  a Galois extension of  $k$  and  $\sigma_1, \sigma_2: L \rightarrow L$  two extensions of  $\sigma: K \rightarrow K$ . Then there exists a unique element  $\tau$  in the Galois group of  $L|K$  such that  $\sigma_2 = \sigma_1\tau$ .*

*Proof.* The uniqueness of  $\tau$  follows from the injectivity of  $\sigma_1$ . Let  $\mathcal{M}$  denote the set of all pairs  $(M, \tau)$  where  $M$  is an intermediate field of  $L|K$  and  $\tau: M \rightarrow L$  a morphism of field extensions of  $K$  satisfying  $\sigma_2(a) = \sigma_1(\tau(a))$  for all  $a \in M$ . By Zorn's Lemma there exists a maximal element  $(M, \tau)$  in  $\mathcal{M}$ . Suppose that  $M$  is properly contained in  $L$ . Choose  $a \in L \setminus M$  and let  $f$  denote the minimal polynomial of  $a$  over  $M$ . Let  ${}^\tau f$  denote the polynomial obtained from  $f$  by applying  $\tau$  to the coefficients. As  $L$  is Galois over  $K$ , we see that  ${}^\tau f$  cannot have a root outside  $L$ . Thus  ${}^\tau f$  has all its roots in  $L$ . Since  $\sigma_2 f = \sigma_1 {}^\tau f$  we see that  $\sigma_1$  maps the roots of  ${}^\tau f$  onto the roots of  $\sigma_2 f$ . As  $\sigma_2(a) \in L$  is a root of  $\sigma_2 f$  this shows that there exists a root  $b \in L$  of  ${}^\tau f$  such that  $\sigma_1(b) = \sigma_2(a)$ . So we can extend  $\tau$  to  $\tau: M(a) \rightarrow L$  by setting  $\tau(a) = b$ ; a contradiction.  $\square$

Let  $k$  be a  $\sigma$ -field and let  $k_s$  denote the separable algebraic closure of  $k$ . Let  $\mathcal{G}$  denote the Galois group of  $k_s|k$ . As noted in Remark 1.11 there exists an extension of  $\sigma: k \rightarrow k$  to an endomorphism of  $k_s$ . Let us fix such an extension. For  $\tau \in \mathcal{G}$  the maps  $\sigma$  and  $\tau\sigma$  are extensions of  $\sigma: k \rightarrow k$  to  $k_s$ . By Lemma 1.20 there exists a unique  $\tau^\sigma \in \mathcal{G}$  such that

$$(1) \quad \tau\sigma = \sigma\tau^\sigma.$$

Then

$$\sigma: \mathcal{G} \rightarrow \mathcal{G}, \tau \mapsto \tau^\sigma$$

is a morphism of groups.

If  $k$  and therefore also  $k_s$  is inversive, this action of  $\sigma$  on the Galois group agrees with the action employed in [Lev08, Section 8.1], where the formula  $\tau^\sigma = \sigma^{-1}\tau\sigma$  is used as the definition.



Note, however, that this formula does not make sense in our context because  $\sigma$  need not be invertible.

The formation of the strong core is compatible with extension of the base  $\sigma$ -field:

**Lemma 1.21.** *Let  $R$  be a  $k$ - $\sigma$ -algebra and  $K$  a  $\sigma$ -field extension  $k$ . Then*

$$\pi_0^\sigma(R \otimes_k K|K) = \pi_0^\sigma(R|k) \otimes_k K.$$

*Proof.* The inclusion “ $\supset$ ” is clear from Lemma 1.8. We will prove the equality in several steps.

Step 1: Assume  $K = k_s$  is the separable algebraic closure of  $k$  equipped with an extension of  $\sigma: k \rightarrow k$ . Let  $\mathcal{G}$  denote the Galois group of  $k_s|k$ . As explained above there is an action of  $\sigma$  on  $\mathcal{G}$  denoted by  $\tau \mapsto \tau^\sigma$ . There also is a natural action of  $\mathcal{G}$  on  $R \otimes_k k_s$  via the right factor:  $\tau(r \otimes \lambda) = r \otimes \tau(\lambda)$  for  $\tau \in \mathcal{G}$ ,  $r \in R$  and  $\lambda \in k$ . For  $f \in R \otimes_k k_s$  and  $\tau \in \mathcal{G}$  we have  $\tau(\sigma(f)) = \sigma(\tau^\sigma(f))$ .

We will show that  $\pi_0^\sigma(R \otimes_k k_s|k_s) \subset R \otimes_k k_s$  is stable under the  $\mathcal{G}$ -action. We know from Lemma 1.18 that  $\pi_0^\sigma(R \otimes_k k_s|k_s)$  is generated as a  $k_s$ -vector space by the periodic idempotent elements of  $R \otimes_k k_s$ . It therefore suffices to show that  $\tau(e)$  is periodic and idempotent for every periodic idempotent element  $e \in R \otimes_k k_s$  and every  $\tau \in \mathcal{G}$ . As  $\tau$  defines an automorphism of  $R \otimes_k k_s$ , clearly also  $\tau(e)$  is idempotent. Assume  $\sigma^n(e) = e$ . For  $i \in \mathbb{N}$  we have

$$(2) \quad \tau(e) = \tau(\sigma^{ni}(e)) = \sigma^{ni}(\tau^{\sigma^{ni}}(e)).$$

Since every orbit of  $\mathcal{G}$  on  $k_s$  is finite, also every orbit of  $\mathcal{G}$  on  $R \otimes_k k_s$  is finite. Therefore  $\{\tau(e), \tau^{\sigma^n}(e), \tau^{\sigma^{2n}}(e), \dots\}$  is a finite set. It follows that there exist  $i < j$  such that  $\tau^{\sigma^{ni}}(e) = \tau^{\sigma^{nj}}(e)$ . Then

$$\tau(e) = \sigma^{ni}(\tau^{\sigma^{ni}}(e)) = \sigma^{ni}(\tau^{\sigma^{nj}}(e)) = \tau^{\sigma^{n(j-i)}}(\sigma^{ni}(e)) = \tau^{\sigma^{n(j-i)}}(e).$$

Thus, replacing  $i$  with  $j - i$  in equation (2), we obtain  $\tau(e) = \sigma^{n(j-i)}(\tau(e))$ . Therefore  $\tau(e)$  is periodic as required.

So  $\pi_0^\sigma(R \otimes_k k_s|k_s) \subset R \otimes_k k_s$  is stable under the  $\mathcal{G}$ -action and it follows from Galois descent ([Bou90, Prop. 6, Chapter V, §10, No. 4, A.V.62] or [Spr09, Prop. 11.1.4, p. 186]) that  $\pi_0^\sigma(R \otimes_k k_s|k_s) = S \otimes_k k_s$ , where  $S$  is the  $k$ - $\sigma$ -subalgebra of  $R$  given by  $S = R \cap \pi_0^\sigma(R \otimes_k k_s|k_s)$ . It now suffices to show that  $k\{s\}$  is strongly  $\sigma$ -étale for every  $s \in S$ . But a finitely  $\sigma$ -generated  $k_s$ - $\sigma$ -subalgebra of  $\pi_0^\sigma(R \otimes_k k_s|k_s)$  is strongly  $\sigma$ -étale, so  $k_s\{s\} = k\{s\} \otimes_k k_s$  is strongly  $\sigma$ -étale and it follows from Lemma 1.8 that  $k\{s\}$  is strongly  $\sigma$ -étale.

Step 2: Assume that  $k = k_s$  is separably algebraically closed and that  $K = \bar{k}$  is the algebraic closure of  $k$ . If the characteristic of  $k$  is zero,  $k_s = \bar{k}$  and there is nothing to prove. So we may assume that the characteristic of  $k$  is  $p > 0$ . Then  $\bar{k}$  is purely inseparable over  $k$ . By Lemma 1.18 it suffices to show that every periodic idempotent element  $e = \sum r_i \otimes \lambda_i \in R \otimes_k \bar{k}$  belongs to  $R$ . As  $\bar{k}$  is purely inseparable over  $k$ , there exists an integer  $n \geq 1$  such that  $\lambda_i^{p^n} \in k$  for all  $i$ . So  $e = e^{p^n} = \sum r_i^{p^n} \otimes \lambda_i^{p^n}$  lies in  $R$ .

Step 3: Assume that  $K = \bar{k}$  is the algebraic closure of  $k$ . Then the separable algebraic closure  $k_s$  of  $k$  is naturally a  $\sigma$ -subfield of  $\bar{k}$  (Remark 1.11) and it follows from steps 2 and 1 that

$$\begin{aligned} \pi_0^\sigma(R \otimes_k \bar{k}|\bar{k}) &= \pi_0^\sigma((R \otimes_k k_s) \otimes_{k_s} \bar{k}|\bar{k}) = \pi_0^\sigma(R \otimes_k k_s|k_s) \otimes_{k_s} \bar{k} = \pi_0^\sigma(R|k) \otimes_k k_s \otimes_{k_s} \bar{k} \\ &= \pi_0^\sigma(R|k) \otimes_k \bar{k}. \end{aligned}$$

Step 4: Assume that  $k$  and  $K$  are algebraically closed. We know from Proposition 1.12 that  $\pi_0^\sigma(R \otimes_k K|K)$  is generated as a  $K$ -vector space by periodic idempotent elements. By Lemma 1.19 every idempotent element  $e$  of  $R \otimes_k K$  is of the form  $e = f \otimes 1$  for some idempotent element

$f \in R$ . If  $e$  is periodic, then also  $f$  is periodic. Therefore  $\pi_0^\sigma(R \otimes_k K|K)$  is generated as a  $K$ -vector space by  $\pi_0^\sigma(R|k)$  and so  $\pi_0^\sigma(R \otimes_k K|K) = \pi_0^\sigma(R|k) \otimes_k K$ .

Step 5: Finally we treat the general case, i.e.,  $K$  is an arbitrary  $\sigma$ -field extension of  $k$ . Let  $\overline{K}$  denote the algebraic closure of  $K$  and choose an extension of  $\sigma: K \rightarrow K$  to  $\overline{K}$ . Then the algebraic closure  $\overline{k}$  of  $k$  is naturally a  $\sigma$ -subfield of  $\overline{K}$ . As  $R \otimes_k \overline{K} = (R \otimes_k \overline{k}) \otimes_{\overline{k}} \overline{K}$  it follows from steps 4 and 3 that

$$\pi_0^\sigma(R \otimes_k \overline{K}|\overline{K}) = \pi_0^\sigma(R \otimes_k \overline{k}|\overline{k}) \otimes_{\overline{k}} \overline{K} = \pi_0^\sigma(R|k) \otimes_k \overline{k} \otimes_{\overline{k}} \overline{K} = \pi_0^\sigma(R|k) \otimes_k K \otimes_K \overline{K}.$$

Moreover,

$$\begin{aligned} \pi_0^\sigma(R|k) \otimes_k K \otimes_K \overline{K} &\subset \pi_0^\sigma(R \otimes_k K|K) \otimes_K \overline{K} \subset \pi_0^\sigma(R \otimes_k K \otimes_K \overline{K}|\overline{K}) = \\ &= \pi_0^\sigma(R \otimes_k \overline{K}|\overline{K}) = \pi_0^\sigma(R|k) \otimes_k K \otimes_K \overline{K}. \end{aligned}$$

Therefore  $(\pi_0^\sigma(R) \otimes_k K) \otimes_K \overline{K} = \pi_0^\sigma(R \otimes_k K) \otimes_K \overline{K}$  and consequently  $\pi_0^\sigma(R|k) \otimes_k K = \pi_0^\sigma(R \otimes_k K|K)$  as desired.  $\square$

The following lemma shows that the formation of  $\pi_0^\sigma(R)$  is compatible with the tensor product.

**Lemma 1.22.** *Let  $R$  and  $S$  be  $k$ - $\sigma$ -algebras. Then*

$$\pi_0^\sigma(R \otimes_k S) = \pi_0^\sigma(R) \otimes_k \pi_0^\sigma(S).$$

*Proof.* The inclusion “ $\supset$ ” follows from the fact that the tensor product of two strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebras is strongly  $\sigma$ -étale (Lemma 1.13).

To prove the inclusion “ $\subset$ ” we may assume that  $k$  is algebraically closed and inversive (Lemma 1.21). We know from Lemma 1.18 that  $\pi_0^\sigma(R \otimes_k S)$  is generated as a  $k$ -vector space by periodic idempotent elements. So let  $e \in R \otimes_k S$  be a periodic idempotent element. It suffices to show that  $e \in \pi_0^\sigma(R) \otimes_k \pi_0^\sigma(S)$ .

For a  $k$ -algebra  $A$ , let  $\pi_0(A)$  denote the union of all étale  $k$ -subalgebras of  $A$ . It follows from [Wat79, Section 6.5] that  $\pi_0(A \otimes_k B) = \pi_0(A) \otimes_k \pi_0(B)$  for  $k$ -algebras  $A$  and  $B$ .

So  $e \in \pi_0(R \otimes_k S) = \pi_0(R) \otimes_k \pi_0(S)$ . Thus there exist étale  $k$ -subalgebras  $R_1$  and  $S_1$  of  $R$  and  $S$  respectively such that  $e \in R_1 \otimes_k S_1$ .

If  $V_i$  is a  $k$ -subspace of  $R$  such that  $e \in V_i \otimes_k S$ , then  $e \in \cap_i (V_i \otimes_k S) = (\cap_i V_i) \otimes_k S$ . Thus there exists a smallest  $k$ -subspace  $V$  of  $R$  such that  $e \in V \otimes_k S$ . Let  $v_1, \dots, v_n$  be a  $k$ -basis of  $V$  and write  $e = \sum v_i \otimes s_i \in V \otimes_k S$ . The idempotent element  $e$  is periodic, say  $\sigma^m(e) = e$ . So  $e = \sum \sigma^m(v_i) \otimes \sigma^m(s_i)$ . By construction of  $V$ , the  $k$ -subspace of  $R$  generated by  $\sigma^m(v_1), \dots, \sigma^m(v_n)$  contains  $V$ . Since  $V$  has dimension  $n$ , this shows that the  $\sigma^m(v_i)$  are a  $k$ -basis of  $V$ . As  $k$  is inversive, we see that  $\sigma^m(V) = V$ . Let  $W = V + \sigma(V) + \dots + \sigma^{m-1}(V)$ . Then  $W$  is a  $k$ -subspace of  $R$  and  $\sigma(W) = W$ . Indeed, for dimension reasons,  $\sigma$  induces a bijection on  $W$ .

As  $V$  is contained in  $R_1$ , every element  $v$  of  $V$  satisfies a separable polynomial over  $k$ . Thus also  $\sigma(v)$  satisfies a separable polynomial over  $k$ . (Cf. the proof of Remark 1.11). It follows that all the elements of  $W$  satisfy separable polynomials over  $k$ . Therefore  $k\{W\} = k[W] \subset R$  is an étale  $k$ -algebra. Because  $k$  is inversive and  $\sigma$  induces a bijection of  $W$ , we see that  $\sigma$  is a bijection on  $k\{W\} = k[W]$ . Thus  $k\{W\}$  is a strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebra. Therefore  $e \in k\{W\} \otimes_k S \subset \pi_0^\sigma(R) \otimes_k S$ .

A similar argument shows that  $e \in R \otimes_k \pi_0^\sigma(S)$  and it follows (using [Bou72, Prop. 7, Chapter I, §2.6, p. 18]) that

$$e \in (\pi_0^\sigma(R) \otimes_k S) \cap (R \otimes_k \pi_0^\sigma(S)) = \pi_0^\sigma(R) \otimes_k \pi_0^\sigma(S).$$

$\square$

**Corollary 1.23.** *The assignment  $R \rightsquigarrow \pi_0^\sigma(R)$  gives rise to a monoidal functor on the category of  $k$ - $\sigma$ -algebras.*

*Proof.* If  $\psi: R \rightarrow S$  is a morphism of  $k$ - $\sigma$ -algebras, it follows from Lemma 1.13 that  $\psi(\pi_0^\sigma(R)) \subset \pi_0^\sigma(S)$ . The compatibility with the tensor product is guaranteed by Lemma 1.22.  $\square$

**1.4. Strong core versus core.** Note that  $\pi_0^\sigma(L|K)$  is a  $\sigma$ -field for an extension of  $\sigma$ -fields  $L|K$ . Our first goal is to compare  $\pi_0^\sigma(L|K)$  to the core of  $L|K$ . Recall ([Lev08, Def. 4.3.17]) that the core

$$\text{Core}(L|K)$$

of an extension of  $\sigma$ -fields  $L|K$  is the union of all intermediate  $\sigma$ -fields of  $L|K$ , whose underlying field is a finite separable field extension of  $K$ . The core  $\text{Core}(L|K)$  is a  $\sigma$ -subfield of  $L$  that plays a fairly prominent role in classical difference algebra, for example in the study of compatibility of  $\sigma$ -field extensions ([Lev08, Theorem 5.4.22]) or in questions related to extending specializations ([Coh65, Theorem XI, Chapter 7]).

**Remark 1.24.** *Let  $L|K$  be a  $\sigma$ -field extension.*

- (i) *We have that  $\pi_0^\sigma(L|K) \subset \text{Core}(L|K)$ .*
- (ii) *If  $L$  is finitely  $\sigma$ -generated over  $K$ ,  $\pi_0^\sigma(L|K)$  is a finite separable field extension of  $K$ .*
- (iii) *We have that  $\pi_0^\sigma(L|K) = \text{Core}(L|K)$  if and only if  $\text{Core}(L|K)$  is  $\sigma$ -separable over  $K$ .*
- (iv) *In particular,  $\pi_0^\sigma(L|K) = \text{Core}(L|K)$  if  $K$  is inversive (Corollary 1.6).*

We will show that in general, for any  $a \in \text{Core}(L|K)$  there exists an  $n \in \mathbb{N}$  such that  $\sigma^n(a) \in \pi_0^\sigma(L|K)$ . Following [Hru04, Def. 4.30] we make the following definition.

**Definition 1.25.** *An extension of  $\sigma$ -fields  $L|K$  is called  $\sigma$ -radicial if for every  $a \in L$  there exists an  $n \in \mathbb{N}$  such that  $\sigma^n(a) \in K$ .*

For example, the inversive closure  $K^*$  ([Lev08, Def. 2.1.6]) of a  $\sigma$ -field  $K$  is a  $\sigma$ -radicial extension of  $K$ . Moreover, every  $\sigma$ -radicial extension of  $K$  is contained in  $K^*$ . For later reference we note the following obvious lemma.

**Lemma 1.26.** *Let  $L|K$  and  $M|L$  be  $\sigma$ -radicial  $\sigma$ -field extensions. Then  $M|K$  is also  $\sigma$ -radicial.*  $\square$

**Lemma 1.27.** *Let  $L|K$  be a finite separable extension of  $\sigma$ -fields. Then  $L$  is  $\sigma$ -radicial over  $\pi_0^\sigma(L|K)$ .*

*Proof.* The sequence of intermediate  $\sigma$ -fields  $K\sigma^i(L)$  of  $L|K$  is decreasing and therefore must stabilize, since  $L|K$  is finite. So there exists an  $n \in \mathbb{N}$  such that  $K\sigma^{n+1}(L) = K\sigma^n(L)$ . The canonical map

$$\begin{aligned} \sigma(K\sigma^n(L)) &= K\sigma^n(L) \otimes_K K \longrightarrow K\sigma^{n+1}(L) = K\sigma^n(L) \\ a \otimes \lambda &\longmapsto \sigma(a)\lambda \end{aligned}$$

is surjective and  $K$ -linear. Thus it is injective and it follows from Proposition 1.2 that  $K\sigma^n(L)$  is  $\sigma$ -separable over  $K$ . Because  $L$  is separable over  $K$ , also  $K\sigma^n(L)$  is separable over  $K$  and we find that  $K\sigma^n(L) \subset \pi_0^\sigma(L|K)$ . Clearly  $L$  is  $\sigma$ -radicial over  $K\sigma^n(L)$ . Thus  $L$  is  $\sigma$ -radicial over  $\pi_0^\sigma(L|K)$ .  $\square$

**Corollary 1.28.** *Let  $L|K$  be an extension of  $\sigma$ -fields. Then  $\text{Core}(L|K)$  is  $\sigma$ -radicial over  $\pi_0^\sigma(L|K)$ .*

*Proof.* Let  $a \in \text{Core}(L|K)$ . Then  $K\langle a \rangle$  is a finite separable  $\sigma$ -field extension of  $K$ . It follows from Lemma 1.27 that there exists an  $n \in \mathbb{N}$  such that  $\sigma^n(a) \in \pi_0^\sigma(K\langle a \rangle|K) \subset \pi_0^\sigma(L|K)$ .  $\square$

The following lemma will be needed in the proof of our enhanced version of Babbitt's decomposition (Theorem 2.8).

**Lemma 1.29.** *Let  $L|K$  be an extension of  $\sigma$ -fields. Then*

$$\pi_0^\sigma(L|\pi_0^\sigma(L|K)) = \pi_0^\sigma(L|K).$$

*Proof.* We abbreviate  $N = \pi_0^\sigma(L|K)$ . Let  $M \subset L$  be a strongly  $\sigma$ -étale  $N$ - $\sigma$ -algebra. We have to show that  $M \subset N$ . By the primitive element theorem, there exists  $a \in M$  such that  $M = N(a)$ . It suffices to show that  $a \in N = \pi_0^\sigma(L|K)$ . Let  $f$  denote the minimal polynomial of  $a$  over  $N$  and let  $g$  denote a polynomial over  $N$  such that  $\sigma(a) = g(a)$ . Let  $N'$  be the  $\sigma$ -field extension  $\sigma$ -generated over  $K$  by the coefficients of  $f$  and  $g$ . Then  $N'$  is strongly  $\sigma$ -étale over  $K$ ,  $N'(a)$  is a  $\sigma$ -field and  $f$  is also the minimal polynomial of  $a$  over  $N'$ . We claim that  $N'(a)$  is strongly  $\sigma$ -étale over  $N'$ . Clearly  $N'(a)$  is étale over  $N'$ . So it suffices to show that  $\sigma(N'(a)) \rightarrow N'(a)$  is injective. Assume that  $f$  has degree  $n$ . Then it suffices to show that  $1, \sigma(a), \dots, \sigma(a^{n-1}) \in L$  are  $N'$ -linearly independent. But this is clearly the case, indeed  $1, \sigma(a), \dots, \sigma(a^{n-1})$  are  $N$ -linearly independent since  $N(a)$  is  $\sigma$ -separable over  $N$ .

So  $N'(a)$  is strongly  $\sigma$ -étale over  $N'$  and  $N'$  is strongly  $\sigma$ -étale over  $K$ . It follows from Lemma 1.14 that  $N'(a)$  is strongly  $\sigma$ -étale over  $K$ . So  $a \in N'(a) \subset \pi_0^\sigma(L|K)$  as claimed.  $\square$

We conclude this section with a result on  $\pi_0^\sigma(L|K)$  for  $\sigma$ -field extensions  $L|K$  that will be needed in the proof of our enhanced version of Babbitt's decomposition theorem (Theorem 2.8). This result also illustrates the importance of the  $\sigma$ -separability assumption. Example 1.32 shows that  $\pi_0^\sigma(L|K)$  is better behaved than  $\text{Core}(L|K)$ .

**Proposition 1.30.** *Let  $L|K$  be an extension of  $\sigma$ -fields such that  $L$  is Galois over  $K$  and let  $M$  be an intermediate  $\sigma$ -field of  $L|K$  that is Galois over  $K$ . Then  $\pi_0^\sigma(L|M)$  is Galois over  $K$ .*

*Proof.* It suffices to show that any finite  $\sigma$ -field extension  $N \subset \pi_0^\sigma(L|M)$  of  $M$  is contained in a finite Galois  $\sigma$ -field extension  $N' \subset \pi_0^\sigma(L|M)$  of  $M$ .

Let  $a \in N$  be such that  $N = M(a)$ . The sequence  $([K(\sigma^i(a)) : K])_{i \in \mathbb{N}}$  is non-increasing and therefore stabilizes. Let  $n \in \mathbb{N}$  be such that  $[K(\sigma^n(a)) : K] = [K(\sigma^i(a)) : K]$  for  $i \geq n$ . Let  $a_1, \dots, a_m \in L$  denote the conjugates of  $\sigma^n(a)$  over  $K$ , where  $a_1 = \sigma^n(a)$ .

Then  $N' = M(a_1, \dots, a_m)$  is a Galois extension of  $K$ . Because  $M(a)$  is  $\sigma$ -separable over  $M$ ,  $\sigma(a)$  has the same degree as  $a$  over  $M$ . So  $M(a) = M(\sigma(a))$ . Inductively, it follows that  $M(a) = M(\sigma^n(a)) \subset N'$ .

We will next show that  $N'$  is a  $\sigma$ -field. It suffices to show that  $\sigma(a_1), \dots, \sigma(a_m) \in N'$ . Let  $f$  denote the minimal polynomial of  $a_1 = \sigma^n(a)$  over  $K$  and let  ${}^\sigma f$  be the polynomial obtained from  $f$  by applying  $\sigma$  to the coefficients. Then  ${}^\sigma f(\sigma^{n+1}(a)) = 0$  and because  $[K(\sigma^{n+1}(a)) : K] = [K(\sigma^n(a)) : K]$ , the polynomial  ${}^\sigma f$  is irreducible. Since  $N'|K$  is Galois and the polynomial  ${}^\sigma f$  has the root  $\sigma(a_1) = \sigma^{n+1}(a_1) \in N'$ , all the roots of  ${}^\sigma f$  lie in  $N'$ . But the roots of  ${}^\sigma f$  are  $\sigma(a_1), \dots, \sigma(a_m)$ . So  $N'$  is a  $\sigma$ -subfield of  $L$ .

It remains to show that  $N'$  is  $\sigma$ -separable over  $M$ . As  $M(a_1) = M(a)$  is  $\sigma$ -separable and finite over  $M$  the canonical map  $\sigma(M(a_1)) = M(a_1) \otimes_M M \rightarrow M(a_1)$  is surjective. So we can write

$$(3) \quad a_1 = \sum_i \sigma(f_i(a_1)) \lambda_i,$$

where the  $f_i$ 's are polynomials over  $M$  and  $\lambda_i \in M$ . Now fix  $j \in \{1, \dots, m\}$  and let  $\tau$  be an element of the Galois group of  $L|K$  that maps  $a_1$  to  $a_j$ . Recall (Equation (1)) that  $\tau(\sigma(b)) = \sigma(\tau^\sigma(b))$  for  $b \in L$ . Applying  $\tau$  to Equation (3) yields

$$(4) \quad a_j = \tau(a_1) = \sum_i \sigma({}^\tau f_i(\tau^\sigma(a_1))) \tau(\lambda_i)$$

where  $\tau^\sigma f_i$  is the polynomial obtained from  $f_i$  by applying  $\tau^\sigma$  to the coefficients. Since  $M$  is Galois over  $K$ , we see that  $\tau^\sigma f_i(\tau^\sigma(a_1)) \in N'$  and  $\tau(\lambda_i) \in M$ . Thus Equation (4) shows that  $a_j$  lies in the image of  $\psi: {}^\sigma(N') = N' \otimes_M M \rightarrow N'$ . Therefore  $\psi$  is surjective and hence also injective. It follows from Proposition 1.2 that  $N'$  is  $\sigma$ -separable over  $M$ .  $\square$

**Corollary 1.31.** *Let  $L|K$  be an extension of  $\sigma$ -fields such that  $L$  is Galois over  $K$ . Then  $\pi_0^\sigma(L|K)$  is Galois over  $K$ .*

*Proof.* This is Proposition 1.30 with  $M = K$ .  $\square$

The following example shows that Corollary 1.31 (and thus also Lemma 1.30) does not remain valid with  $\text{Core}(L|K)$  in place of  $\pi_0^\sigma(L|K)$ . In other words, if  $L|K$  is an extension of  $\sigma$ -fields such that  $L$  is Galois over  $K$ , then  $\text{Core}(L|K)$  need not be Galois over  $K$ .

**Example 1.32.** We use the theory of the limit degree and benign extensions explained in Section 2. Let  $x, y, z$  denote  $\sigma$ -variables over  $\mathbb{C}$ , where we consider  $\mathbb{C}$  as a  $\sigma$ -field by virtue of the identity map. We fix an extension of  $\sigma: \mathbb{C}\langle x, y, z \rangle \rightarrow \mathbb{C}\langle x, y, z \rangle$  to the algebraic closure  $L$  of  $\mathbb{C}\langle x, y, z \rangle$ . The polynomial  $f = T^3 + xT^2 + yT + z$  has Galois group  $S_3$  over  $\mathbb{C}\langle x, y, z \rangle$ . Let  $a, b, c \in L$  denote the roots of  $f$ . Then  $\mathbb{C}\langle x, y, z \rangle\langle a, b, c \rangle$  is benign over  $\mathbb{C}\langle x, y, z \rangle$  with limit degree 6. Let  $K = \mathbb{C}\langle x, y, z \rangle\langle \sigma(a) \rangle$ . Then  $K(a)$  is a  $\sigma$ -field extension of  $K$  and therefore  $a \in \text{Core}(L|K)$ . The element  $b \in L$  is conjugate with  $a$  over  $K$  but  $K\langle b \rangle$  is not a finite extension of  $K$ . Thus  $b \notin \text{Core}(L|K)$ . This shows that  $\text{Core}(L|K)$  is not Galois.

## 2. BABBITT'S DECOMPOSITION

Babbitt's decomposition is an important structure theorem for finitely  $\sigma$ -generated extensions of  $\sigma$ -fields  $L|K$  such that  $L|K$  is Galois (as a field extension). See [Bab62, Theorem 2.3] or [Lev08, Theorem 5.4.13]. In the original formulation it is assumed that the base  $\sigma$ -field  $K$  is inversive. Here we will show that this assumption is not necessary. In [Tom16] and [Tom15], the author has shown how to use Babbitt's decomposition for  $K$  not necessarily inversive, by imposing the assumption that  $L|K$  be  $\sigma$ -separable, but in the present paper we proceed in a more elegant way.

Our overall strategy of proof is similar to Babbitt's. However, the original proof uses the assumption that  $K$  is inversive in various places and therefore several changes and complements are necessary. We use  $\pi_0^\sigma(L|K)$  rather than  $\text{Core}(L|K)$ , as well as the notion of a substandard generator rather than the notion of a standard generator (see Definitions 2.1 and 2.2 below). Consequently, the overall structure of the proof now appears somewhat clearer, because we do not need to make the extra step of passing to the inversive closure in order to be able to apply the induction hypothesis.

The proof of Babbitt's decomposition is by induction on a numerical invariant called the limit degree. Let us recall the definition (see [Lev08, Section 4.3] or [Coh65, Chapter 5, Section 16, p. 135]).

Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields, say  $L = K\langle F \rangle$ , with  $F \subset L$  finite. For  $i \in \mathbb{N}$  let

$$(5) \quad d_i = [K(F, \sigma(F), \dots, \sigma^i(F)) : K(F, \sigma(F), \dots, \sigma^{i-1}(F))].$$

Then the sequence  $(d_i)_{i \in \mathbb{N}}$  is non-increasing and therefore stabilizes. The eventual value  $\text{ld}(L|K) = \lim_{i \rightarrow \infty} d_i$  does not depend on the choice of  $F$  and is called the *limit degree* of  $L|K$ .

An extension  $L|K$  of  $\sigma$ -fields is called *benign* ([Lev08, Def. 5.4.7]) if there exists an intermediate field  $K \subset M \subset L$  such that  $M$  is finite and Galois over  $K$  with  $L = K\langle M \rangle$  and  $\text{ld}(L|K) = [M : K]$ . Assuming that  $M$  is finite and Galois with  $L = K\langle M \rangle$ , the condition

$\text{ld}(L|K) = [M : K]$  is equivalent to the condition that  $[K(\sigma^i(M)) : K] = [M : K]$  for all  $i \in \mathbb{N}$  and the fields  $(K(\sigma^i(M)))_{i \in \mathbb{N}}$  are linearly disjoint over  $K$ . If  $L|K$  is benign, then  $L|K$  is Galois and finitely  $\sigma$ -generated.

We also recall the notion of a standard generator ([Lev08, Def. 5.4.5] or [Coh65, p. 217]).

**Definition 2.1.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois. An element  $a \in L$  is called a standard generator of  $L|K$  if the following properties are satisfied:*

- $K\langle a \rangle = L$ .
- $[K(a, \sigma(a)) : K(a)] = \text{ld}(L|K)$ .
- The field extension  $K(a)|K$  is Galois.

A minimal standard generator  $a$  of  $L|K$  is a standard generator  $a$  of  $L|K$  such that  $[K(a) : K] \leq [K(b) : K]$  for every standard generator  $b$  of  $L|K$ .

**Definition 2.2.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois. An element  $a \in L$  is called a substandard generator of  $L|K$  if the following properties are satisfied:*

- $L$  is  $\sigma$ -radicial over  $K\langle a \rangle$ .
- $[K(a, \sigma(a)) : K(a)] = \text{ld}(L|K)$ .
- The field extension  $K(a)|K$  is Galois.

A minimal substandard generator  $a$  of  $L|K$  is a substandard generator  $a$  of  $L|K$  such that  $[K(a) : K] \leq [K(b) : K]$  for every substandard generator  $b$  of  $L|K$ .

As explained on page 334 in [Lev08], for any finitely  $\sigma$ -generated extension of  $\sigma$ -fields  $L|K$  such that  $L|K$  is Galois, there exists a standard generator of  $L|K$ . In particular, there exists a minimal substandard generator.

Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois and let  $a$  be a minimal standard generator of  $L|K$ . As the sequence of the  $d_i$ 's (Equation (5)) is non-increasing, we have

$$[K(a) : K] \geq [K(a, \sigma(a)) : K(a)] = \text{ld}(L|K).$$

**Lemma 2.3.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois and let  $a$  be a minimal standard generator of  $L|K$ . Then  $L|K$  is benign if and only if  $[K(a) : K] = \text{ld}(L|K)$ .*

*Proof.* Assume that  $L|K$  is benign and let  $M \subset L$  be a finite Galois extension of  $K$  such that  $\text{ld}(L|K) = [M : K]$ . Choose  $b \in M$  such that  $M = K(b)$ . Then  $b$  is a minimal standard generator of  $L|K$  and  $[K(b) : K] = \text{ld}(L|K)$ .

Conversely, if  $a$  is a minimal standard generator of  $L|K$  with  $[K(a) : K] = \text{ld}(L|K)$ , then  $M = K(a) \subset L$  is a Galois extension of  $K$  with  $K\langle M \rangle = L$  and  $\text{ld}(L|K) = [M : K]$ .  $\square$

**Corollary 2.4.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois and let  $a$  be a minimal substandard generator of  $L|K$ . If  $[K(a) : K] = \text{ld}(L|K)$ , then  $K\langle a \rangle|K$  is benign.*

*Proof.* A finitely  $\sigma$ -generated extension of  $\sigma$ -fields has limit degree one if and only if it is finitely generated as a field extension ([Coh65, Theorem XV, Chapter 5, p. 143]). A finitely  $\sigma$ -generated  $\sigma$ -radicial extension of  $\sigma$ -fields is finitely generated as a field extension and therefore has limit degree one. So  $\text{ld}(L|K\langle a \rangle) = 1$ . Using the multiplicativity of the limit degree ([Lev08, Theorem 4.3.4]) we find

$$\text{ld}(L|K) = \text{ld}(L|K\langle a \rangle) \cdot \text{ld}(K\langle a \rangle|K) = \text{ld}(K\langle a \rangle|K).$$

So a standard generator of  $K\langle a \rangle$  over  $K$  is a substandard generator of  $L$  over  $K$ . Therefore  $a$  is a minimal standard generator of  $K\langle a \rangle$  over  $K$  and it follows from Lemma 2.3 that  $K\langle a \rangle|K$  is benign.  $\square$

**Lemma 2.5.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois and let  $a$  be a substandard generator of  $L|K$ . Then also  $\sigma(a)$  is a substandard generator of  $L|K$ . Moreover, if  $a$  is a minimal substandard generator of  $L|K$  then  $[K(\sigma(a)) : K] = [K(a) : K]$ .*

*Proof.* Because  $L|K\langle a \rangle$  and  $K\langle a \rangle|K\langle \sigma(a) \rangle$  are  $\sigma$ -radical, also  $L|K\langle \sigma(a) \rangle$  is  $\sigma$ -radical (Lemma 1.26).

If  $f \in K(a)[x]$  is the minimal polynomial of  $\sigma(a)$  over  $K(a)$ , then  $\sigma f(\sigma^2(a)) = 0$  and  $\sigma f \in K(\sigma(a))[x]$ . Thus the degree of  $\sigma^2(a)$  over  $K(\sigma(a))$  is less than or equal to the degree of  $\sigma(a)$  over  $K(a)$ . Therefore

$$[K(\sigma(a), \sigma^2(a)) : K(\sigma(a))] \leq [K(a, \sigma(a)) : K(a)] = \text{ld}(L|K).$$

On the other hand,  $[K(\sigma(a), \sigma^2(a)) : K(\sigma(a))] \geq \text{ld}(K\langle \sigma(a) \rangle|K)$  and (as in the proof of Corollary 2.4)

$$\text{ld}(L|K) = \text{ld}(L|K\langle \sigma(a) \rangle) \cdot \text{ld}(K\langle \sigma(a) \rangle|K) = \text{ld}(K\langle \sigma(a) \rangle|K).$$

Therefore  $[K(\sigma(a), \sigma^2(a)) : K(\sigma(a))] = \text{ld}(L|K)$ . Finally  $K(\sigma(a))|K$  is Galois because  $K(a)|K$  is Galois. So  $\sigma(a)$  is a substandard generator of  $L|K$ .

If we assume that  $a$  is a minimal substandard generator of  $L|K$ , the fact that also  $\sigma(a)$  is a substandard generator of  $L|K$ , implies that  $[K(a) : K] \leq [K(\sigma(a)) : K]$  and so  $[K(a) : K] = [K(\sigma(a)) : K]$ .  $\square$

**Lemma 2.6.** *Let  $L|K$  be a finitely  $\sigma$ -generated extension of  $\sigma$ -fields such that  $L|K$  is Galois and let  $a$  be a minimal substandard generator of  $L|K$ . Let  $b \in K(a)$  with  $b \notin K$ . Then  $\sigma^i(b) \notin K$  for  $i \in \mathbb{N}$ .*

*Proof.* By Lemma 2.5 we have  $[K(\sigma^i(a)) : K] = [K(a) : K]$  for any  $i \in \mathbb{N}$ . So

$$1, \sigma^i(a), \sigma^i(a)^2, \dots, \sigma^i(a)^{n-1}$$

are  $K$ -linearly independent, where  $n$  is the degree of  $a$  over  $K$ . Write  $b = b_0 + b_1a + \dots + b_{n-1}a^{n-1}$  with  $b_0, \dots, b_{n-1} \in K$ . Then

$$\sigma^i(b) = \sigma^i(b_0) + \sigma^i(b_1)\sigma^i(a) + \dots + \sigma^i(b_{n-1})\sigma^i(a)^{n-1}.$$

Suppose  $\sigma^i(b) \in K$ . Because  $1, \sigma^i(a), \sigma^i(a)^2, \dots, \sigma^i(a)^{n-1}$  are  $K$ -linearly independent, it follows that  $\sigma^i(b) = \sigma^i(b_0)$ . So  $b = b_0 \in K$ , in contradiction to the assumption  $b \notin K$ .  $\square$

**Lemma 2.7.** *Let  $L|K$  be a  $\sigma$ -radical extension of  $\sigma$ -fields and  $a_1, \dots, a_n$  elements in a  $\sigma$ -field extension of  $L$  such that  $L\langle a_1, \dots, a_i \rangle$  is benign over  $L\langle a_1, \dots, a_{i-1} \rangle$  with minimal standard generator  $a_i$  for  $i = 1, \dots, n$ . Then there exist integers  $r_1, \dots, r_n \geq 0$  such that  $K\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_i}(a_i) \rangle$  is benign over  $K\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_{i-1}}(a_{i-1}) \rangle$  with minimal standard generator  $\sigma^{r_i}(a_i)$  for  $i = 1, \dots, n$ .*

*Proof.* We first treat the case  $n = 1$ . So  $a := a_1$  is a minimal standard generator of  $L\langle a \rangle$  over  $L$ . We claim that  $K\langle \sigma^j(a) \rangle|K$  is benign with minimal standard generator  $\sigma^j(a)$  for  $j \gg 0$ .

Let  $f$  denote the minimal polynomial of  $a$  over  $L$ . Because  $L(a)$  is the splitting field of  $f$ , every root of  $f$  can be written as a polynomial in  $a$  with coefficients in  $L$ . Since  $L|K$  is  $\sigma$ -radical, every root of  $\sigma^j f$  can be written as a polynomial in  $\sigma^j(a)$  with coefficients in  $K$  for  $j \gg 0$ . Therefore  $K(\sigma^j(a))$  is the splitting field of  $\sigma^j f$  for  $j \gg 0$ . Because  $f$  is separable also  $\sigma^j f$  is separable. Therefore  $K(\sigma^j(a))|K$  is Galois.

Because  $L$  is  $\sigma$ -radicial over  $K$  there exists an integer  $i$  such that  $\sigma^j f$  has coefficients in  $K$  for  $j \geq i$ . It suffices to show that  $\sigma^{j+l} f$  is irreducible over  $K(\sigma^j(a), \dots, \sigma^{j+l-1}(a))$  for  $l \in \mathbb{N}$  and  $j \geq i$ . Suppose the contrary. Then  $\sigma^{j+l} f$  is reducible over  $L(a, \dots, \sigma^{j+l-1}(a))$ . This contradicts the fact that  $L\langle a \rangle|L$  is benign with minimal standard generator  $a$ . This finishes the case  $n = 1$ .

The general case now follows from the  $n = 1$  case by induction, with  $K\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_{n-1}}(a_{n-1}) \rangle$  in place of  $K$  and  $L\langle a_1, \dots, a_{n-1} \rangle$  in place of  $L$ .  $\square$

Now we are prepared to prove the enhanced version of Babbitt's decomposition theorem.

**Theorem 2.8.** *Let  $K$  be a  $\sigma$ -field and  $L$  a finitely  $\sigma$ -generated  $\sigma$ -field extension of  $K$  such that  $L|K$  is Galois. Then there exists a chain of intermediate  $\sigma$ -fields*

$$K \subset L_0 \subset L_1 \subset \dots \subset L_{n-1} \subset L_n \subset L$$

such that  $L_0 = \pi_0^\sigma(L|K)$ ,  $L_i$  is benign over  $L_{i-1}$  for  $i = 1, \dots, n$  and  $L$  is  $\sigma$ -radicial over  $L_n$ .

*Proof.* The proof is by induction on  $\text{ld}(L|K)$ . If  $\text{ld}(L|K) = 1$ , then  $L|K$  is finite ([Coh65, Theorem XVII, p. 144]). Thus, in this case, the claim follows from Lemma 1.27. So we can assume that  $\text{ld}(L|K) > 1$ . Replacing  $K$  with  $\pi_0^\sigma(L|K)$ , we can assume that  $\pi_0^\sigma(L|K) = K$  (Lemma 1.29).

First, we also assume that  $L|K$  contains no intermediate  $\sigma$ -field  $M$  such that  $M|K$  is Galois and  $1 < \text{ld}(M|K) < \text{ld}(L|K)$ . We will show that the theorem holds with  $n = 1$ .

Let  $a$  be a minimal substandard generator of  $L|K$ . Then  $K(a)$  and  $K(\sigma(a))$  are Galois extensions of  $K$ . Therefore (see e.g., [Coh65, Theorem VI, p. 6])

$$[K(a, \sigma(a)) : K] = \frac{[K(a) : K] \cdot [K(\sigma(a)) : K]}{[K(a) \cap K(\sigma(a)) : K]}.$$

On the other hand,

$$[K(a, \sigma(a)) : K] = [K(a, \sigma(a)) : K(a)] \cdot [K(a) : K] = \text{ld}(L|K) \cdot [K(a) : K].$$

Because  $[K(\sigma(a)) : K] = [K(a) : K]$  by Lemma 2.5, the last two equations yield

$$[K(a) : K] = \text{ld}(L|K) \cdot [K(a) \cap K(\sigma(a)) : K].$$

Since  $\text{ld}(L|K) > 1$ , we see that  $[K(a) \cap K(\sigma(a)) : K] < [K(a) : K]$ .

Let  $b$  be a primitive element of  $K(a) \cap K(\sigma(a))$  over  $K$ . Then  $[K(b) : K] < [K(a) : K]$  and  $K(b)|K$  is Galois. Therefore also  $K\langle b \rangle|K$  is Galois. By assumption,  $\text{ld}(K\langle b \rangle|K) = 1$  or  $\text{ld}(K\langle b \rangle|K) = \text{ld}(L|K)$ .

Let us first assume that  $\text{ld}(K\langle b \rangle|K) = \text{ld}(L|K)$ . Then

$$[K(b, \sigma(b)) : K(b)] \geq \text{ld}(K\langle b \rangle|K) = \text{ld}(L|K)$$

and therefore

$$[K(b, \sigma(b)) : K] = [K(b, \sigma(b)) : K(b)] \cdot [K(b) : K] \geq \text{ld}(L|K) \cdot [K(a) \cap K(\sigma(a)) : K].$$

But  $K(b, \sigma(b)) \subset K(\sigma(a))$  and so

$$[K(b, \sigma(b)) : K] \leq [K(\sigma(a)) : K] = [K(a) : K] = \text{ld}(L|K) \cdot [K(a) \cap K(\sigma(a)) : K].$$

Thus  $K(b, \sigma(b)) = K(\sigma(a))$  and  $[K(b, \sigma(b)) : K(b)] = \text{ld}(L|K)$ . So  $K\langle b \rangle = K\langle \sigma(a) \rangle$ ,  $L$  is  $\sigma$ -radicial over  $K\langle b \rangle$  and  $b$  is a substandard generator of  $L|K$ . Since  $[K(b) : K] < [K(a) : K]$ , this contradicts the fact that  $a$  is a minimal substandard generator of  $L|K$ .

Hence  $\text{ld}(K\langle b \rangle|K) = 1$ . Because  $\pi_0^\sigma(L|K) = K$ , it follows from Corollary 1.28 that  $\sigma^n(b) \in K$  for some  $n \in \mathbb{N}$ . But then  $b \in K$  by Lemma 2.6. So  $K(a) \cap K(\sigma(a)) = K$  and  $[K(a) : K] =$



$\text{ld}(L|K)$ . Thus  $K\langle a \rangle|K$  is benign by Corollary 2.4. Because  $L|K\langle a \rangle$  is  $\sigma$ -radicial, we see that the theorem is satisfied with  $n = 1$  and  $L_1 = K\langle a \rangle$ .

Now we assume that there exists an intermediate  $\sigma$ -field  $K \subset M \subset L$  such that  $M|K$  is Galois and  $1 < \text{ld}(M|K) < \text{ld}(L|K)$ . We know from Proposition 1.30 that  $\pi_0^\sigma(L|M)$  is Galois over  $K$ . Moreover

$$\text{ld}(\pi_0^\sigma(L|M)|K) = \text{ld}(\pi_0^\sigma(L|M)|M) \cdot \text{ld}(M|K) = \text{ld}(M|K).$$

Replacing  $M$  with  $\pi_0^\sigma(L|M)$ , we may assume that  $\pi_0^\sigma(L|M) = M$  (Lemma 1.29). By Theorem [Lev08, Theorem 4.4.1, p. 292] an intermediate  $\sigma$ -field of a finitely  $\sigma$ -generated  $\sigma$ -field extension is finitely  $\sigma$ -generated. So  $M$  is finitely  $\sigma$ -generated over  $K$ . Applying the induction hypothesis to  $M|K$  yields a sequence of  $\sigma$ -fields

$$K \subset L_1 \subset \cdots \subset L_n \subset M,$$

where the extensions  $L_1|K$  and  $L_i|L_{i-1}$  ( $2 \leq i \leq n$ ) are benign and  $M|L_n$  is  $\sigma$ -radicial. Applying the induction hypothesis to  $L|M$  yields a sequence of  $\sigma$ -fields

$$M \subset M_1 \subset \cdots \subset M_m \subset L,$$

where the extensions  $M_1|M$  and  $M_i|M_{i-1}$  ( $2 \leq i \leq m$ ) are benign and  $L|M_m$  is  $\sigma$ -radicial.

Let  $a_1$  be a minimal standard generator of  $M_1|M$  and for  $i = 2, \dots, m$  let  $a_i \in M_i$  be a minimal standard generator of  $M_i|M_{i-1}$ . As  $M|L_n$  is  $\sigma$ -radicial, by Lemma 2.7 there exist  $r_1, \dots, r_m \in \mathbb{N}$  such that  $L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_i}(a_i) \rangle$  is benign over  $L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_{i-1}}(a_{i-1}) \rangle$  for  $i = 1, \dots, m$ .

We have constructed a sequence of benign  $\sigma$ -field extensions

$$K \subset L_1 \subset \cdots \subset L_n \subset L_n\langle \sigma^{r_1}(a_1) \rangle \subset \cdots \subset L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_m}(a_m) \rangle$$

inside  $L$ . It remains to see that  $L$  is  $\sigma$ -radicial over  $L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_m}(a_m) \rangle$ . But  $L$  is  $\sigma$ -radicial over  $M_m$  and  $M_m = M\langle a_1, \dots, a_m \rangle$  is  $\sigma$ -radicial over  $L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_m}(a_m) \rangle$ . Therefore  $L$  is  $\sigma$ -radicial over  $L_n\langle \sigma^{r_1}(a_1), \dots, \sigma^{r_m}(a_m) \rangle$ .  $\square$

**Remark 2.9.** *Let us summarize, using the notation of Theorem 2.8, the features that make our version of Babbitt's decomposition more versatile than the original.*

- (i) *As already mentioned, it applies to difference field extensions  $L|K$  where the base field  $K$  is not necessarily inversive.*
- (ii) *We make the relationship of  $L_n$  and  $L$  explicit. Indeed, in our version, the tower  $K \subset L_n \subset L$  gives a decomposition of  $L|K$  into a  $\sigma$ -separable part and a  $\sigma$ -radicial part, whereas the original theorem only asserts that the inversive closures of  $L_n$  and  $L$  coincide.*

### 3. APPLICATIONS

**3.1. A contribution to the study of difference algebraic groups.** As mentioned in the introduction, an initial motivation for studying strongly  $\sigma$ -étale  $k$ - $\sigma$ -algebras is their use for understanding the difference connected components of difference algebraic groups. In this article we do not want to go through the details of the definition of a difference algebraic group. (The interested reader is referred to [Wib] and [Wib15].) We simply rely on the fact that the category of difference algebraic groups is anti-equivalent to the category of  $k$ - $\sigma$ -Hopf algebras that are finitely  $\sigma$ -generated as  $k$ - $\sigma$ -algebras ([Wib, Prop. 2.3]). Here a  $k$ - $\sigma$ -algebra  $R$  with the structure of a Hopf algebra over  $k$  is called a  *$k$ - $\sigma$ -Hopf algebra* if the structure maps of the Hopf algebra, i.e., the comultiplication  $\Delta: R \rightarrow R \otimes_k R$ , the antipode  $S: R \rightarrow R$  and the counit  $\varepsilon: R \rightarrow k$ , are morphisms of difference rings.

**Fact 3.1** ([Wib, Theorem 4.5]). *A  $k$ - $\sigma$ -Hopf subalgebra of a  $k$ - $\sigma$ -Hopf algebra which is finitely  $\sigma$ -generated over  $k$ , is finitely  $\sigma$ -generated over  $k$ .*

**Theorem 3.2.** *Let  $R$  be a  $k$ - $\sigma$ -Hopf algebra. Then  $\pi_0^\sigma(R)$  is a  $k$ - $\sigma$ -Hopf subalgebra of  $R$ . Moreover, if  $R$  is finitely  $\sigma$ -generated over  $k$ , then  $\pi_0^\sigma(R)$  is strongly  $\sigma$ -étale over  $k$ .*

*Proof.* The first claim is immediate using Corollary 1.23, and the second follows from Fact 3.1.  $\square$

**Remark 3.3.** *Let  $R$  be a  $k$ - $\sigma$ -algebra and let  $S$  be the union of all  $k$ - $\sigma$ -subalgebras of  $R$  that are étale as  $k$ -algebras. The following example shows that*

- (i)  *$S$  need not be finitely  $\sigma$ -generated over  $k$ , even if  $R$  is;*
- (ii) *if  $R$  is a  $k$ - $\sigma$ -Hopf algebra,  $S$  need not be a  $k$ - $\sigma$ -Hopf subalgebra of  $R$ .*

*Thus, working with strongly  $\sigma$ -étale algebras (and the condition of  $\sigma$ -separability) in the definition of  $\pi_0^\sigma$  is crucial for Conjecture 1.17, for obtaining nice functorial properties from Corollary 1.23, and for Theorem 3.2.*

**Example 3.4.** A geometrically more intuitive description of this example can be found in [Wib15, Ex. 4.2.15]. We refer the reader to Sections 2.2 and 2.3 in [Lev08] for definitions and basic constructions regarding difference polynomial ideals.

Let  $R_1 = k\{y\}/[y^2 - 1, \sigma(y) - 1]$  denote the quotient of the univariate  $\sigma$ -polynomial ring modulo the  $\sigma$ -ideal  $\sigma$ -generated by  $y^2 - 1$  and  $\sigma(y) - 1$ . Similarly, let  $R_2 = k\{y\}/[y^2 - 1]$ . If we denote by  $z$  the image of  $y$  in  $R_1$  respectively  $R_2$ , one may check that the formulas  $\Delta(z) = z \otimes z$ ,  $S(z) = z$  and  $\varepsilon(z) = 1$  define the structure of a  $k$ - $\sigma$ -Hopf algebra on  $R_1$  respectively  $R_2$ . So  $R = R_1 \otimes_k R_2$ , equipped with the product Hopf algebra structure, is naturally a  $k$ - $\sigma$ -Hopf algebra.

Let  $S$  be the union of all  $k$ - $\sigma$ -subalgebras of  $R$  that are étale as  $k$ -algebras. Let us assume that the characteristic of  $k$  is not equal to 2, so that  $R$  is a union of étale  $k$ -algebras. We have  $R_1 = ke_1 \oplus ke_2$  for orthogonal idempotent elements  $e_1, e_2 \in R_1$  with  $\sigma(e_1) = 1$  and  $\sigma(e_2) = 0$ . So

$$R = R_1 \otimes_k R_2 = (e_1 \otimes R_2) \oplus (e_2 \otimes R_2).$$

For any element  $a \in e_2 \otimes R_2$  we have  $\sigma(a) = 0$  and so  $k\{a\} = k[a]$  is an étale  $k$ -algebra. This shows that  $e_2 \otimes R_2$  is contained in  $S$ . In particular,  $S$  has infinite dimension as a  $k$ -vector space. Thus,  $S$  is not finitely  $\sigma$ -generated over  $k$ , and Fact 3.1 shows that it is not a  $k$ - $\sigma$ -Hopf subalgebra of  $R$ . On the other hand,  $\pi_0^\sigma(R) = k$ .

**3.2. An application to compatibility.** Recall ([Lev08, Def. 5.1.1]) that two extensions of  $\sigma$ -fields  $L|K$  and  $L'|K$  are called *compatible* if there exists a  $\sigma$ -field extension of  $K$  that contains isomorphic copies of  $L|K$  and  $L'|K$ .

The classical compatibility theorem ([Lev08, Theorem 5.4.22]) states that two extensions of  $\sigma$ -fields are compatible if and only if their cores are compatible. We will improve on this by showing that the core can be replaced by  $\pi_0^\sigma$ . Note that for a  $\sigma$ -field extension  $L|K$  one has  $\pi_0^\sigma(L|K) \subset \text{Core}(L|K)$ .

**Lemma 3.5.** *Let  $L|K$  and  $L'|K$  be two extensions of  $\sigma$ -fields. If  $L|K$  is  $\sigma$ -radicial then  $L|K$  and  $L'|K$  are compatible.*

*Proof.* Let  $L'^*$  denote the inversive closure of  $L'$ . (See [Lev08, Def. 2.1.6].) Then  $L'^*$  contains an inversive closure of  $K$ . On the other hand, because  $L|K$  is  $\sigma$ -radicial, the inversive closure  $L^*$  of  $L$  is an inversive closure of  $K$ . So, by the uniqueness of the inversive closure, there exists a  $K$ -embedding of  $L^*$  into  $L'^*$ , which restricts to a  $K$ -embedding of  $L$  into  $L'^*$ . Thus  $L'^*$  contains isomorphic copies of  $L|K$  and  $L'|K$ .  $\square$

**Theorem 3.6.** *Let  $L|K$  and  $L'|K$  be two extensions of  $\sigma$ -fields. Then  $L|K$  and  $L'|K$  are compatible if and only if  $\pi_0^\sigma(L|K)|K$  and  $\pi_0^\sigma(L'|K)|K$  are compatible.*

*Proof.* A possible line of proof would be to follow the proof of the classical compatibility theorem, but to use Theorem 2.8 instead of the classical version of Babbitt's decomposition. However, using Corollary 1.28 and Lemma 3.5, we can easily deduce a proof from the classical compatibility theorem:

A  $\sigma$ -field extension containing isomorphic copies of  $L|K$  and  $L'|K$  obviously also contains isomorphic copies of  $\pi_0^\sigma(L|K)|K$  and  $\pi_0^\sigma(L'|K)|K$ . To prove the non-trivial implication, it suffices, by the classical compatibility theorem, to show that  $\text{Core}(L|K)$  and  $\text{Core}(L'|K)$  are compatible. By assumption, there exists a  $\sigma$ -field extension  $M$  of  $K$ , containing  $\pi_0^\sigma(L|K)|K$  and  $\pi_0^\sigma(L'|K)|K$ . By Corollary 1.28 and Lemma 3.5 there exists a  $\sigma$ -field extension  $M_1$  of  $\pi_0^\sigma(L|K)$  containing  $M$  and  $\text{Core}(L|K)$ . Similarly, by Corollary 1.28 and Lemma 3.5 there exists a  $\sigma$ -field extension  $M_2$  of  $\pi_0^\sigma(L'|K)$  containing  $M_1$  and  $\text{Core}(L'|K)$ . Thus  $M_2$  contains  $\text{Core}(L|K)$  and  $\text{Core}(L'|K)$ .  $\square$

## REFERENCES

- [Bab62] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.
- [Bou72] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris, 1972. Translated from the French.
- [Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.
- [CHP02] Zoé Chatzidakis, Ehud Hrushovski, and Ya'acov Peterzil. Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc.* (3), 85(2):257–311, 2002.
- [Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.
- [DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.
- [Hru04] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms, 2004. arXiv:math/0406514v1, updated version available from <http://www.ma.huji.ac.il/~ehud/>.
- [Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
- [Mil12] James S. Milne. Basic theory of affine group schemes, 2012. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [Spr09] T. A. Springer. *Linear algebraic groups*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, second edition, 2009.
- [Sta14] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>, 2014.
- [Tom14] Ivan Tomašić. Direct twisted Galois stratification. arXiv:1412.8066, 2014. Submitted.
- [Tom15] Ivan Tomašić. Galois stratification and ACFA. *Ann. Pure Appl. Logic*, 166(5):639–663, 2015.
- [Tom16] Ivan Tomašić. Twisted Galois stratification. arXiv:1112.0802, 2016. To appear in Nagoya Math J.
- [Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.
- [Wib] Michael Wibmer. Affine difference algebraic groups. arXiv:1405.6603.
- [Wib10] Michael Wibmer. *Geometric difference Galois theory*. PhD thesis, Heidelberg, 2010. <http://www.ub.uni-heidelberg.de/archiv/10685>.
- [Wib15] Michael Wibmer. Affine difference algebraic groups, 2015. Habilitation thesis, available at <http://www.math.upenn.edu/~wibmer/habilWibmer.pdf>.

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY UNIVERSITY OF LONDON, E1 4NS, UK  
*E-mail address:* i.tomasic@qmul.ac.uk

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA PA 19104-6395, USA  
*E-mail address:* wibmer@math.upenn.edu